

Meeting Summary

eHealth Technical Working Group

February 1, 2010 12:30-2:00PM

Please refer to the draft straw man architecture document for additional information.

Review of Changes to the Draft Architecture:

Walter went over the changes that had been made in the latest version (1/25) of the draft straw man architecture. Based on feedback from the TAC, individual providers and other users are no longer part of the registry service or the authentication service. The following changes have been made:

- What was previously known as the Registry Service has been renamed the Entity Registry Service. Whereas previously, the registry included entries for any principal, it now contains only entries for entities, which are the organizations to which the providers belong. The authentication and provisioning of the individual providers is now being delegated to those entities, rather than being handled by the core services.
- What was known as the Routing Service is now being called the Provider Directory Service. This service, which was originally intended to contain a comprehensive directory of principals and their network addresses, is now optional and may be used by an entity that either cannot or chooses not to host and maintain its own directory of providers.
- The previous Authentication Service, which originally was described as authenticating all principals, is now an optional service called the Provider Identity Service that exists for the benefit of any entity that either cannot or chooses not to authenticate its own users in a trusted fashion. The Provider Identity Service consists of a body that certifies provider identities, distributes credentials to those providers, performs authentication during login, and generates authentication assertions needed for the relevant transactions.

An implication of this design decision is that entities who do not use the optional Provider Directory or Authentication Services will trust each other to reliably manage and authenticate their users. For a given HIE transaction, the entity will provide an assertion that it has authenticated the user and vouches for the user's identity. Each entity making the assertion will necessarily have an entry in the Entity Registry Service, which means that the identity of the entity itself has been vetted and provisioned by a central certificate authority that is part of the cooperative shared infrastructure.

There was a brief discussion about the revised trust framework, during which the following points were raised.

- Revised trust framework
 - A key question asked by some members of TWG is whether the revised trust framework as described would be sufficient for organizations (and in particular, large organizations) to participate in HIE through CS-HIE services due to potential liability concerns now that more responsibility would be placed on the entities to credential and authenticate their

own users. The opinion of TAC is that compared to the original individual-level trust framework, a framework based on system-level trust would be sufficient to enable HIE, while posing a lower barrier to adoption for institutions already capable of managing their own users.

- Walter and Rim noted that the framework appears to comply with the privacy and security guidelines that Cal PSAB has recommended; thus, the legal permissibility of the framework should not be an issue.
- The Provider Identity Service offers a “safety valve” mechanism to the trust issue, providing a way to certify individual providers for organizations that otherwise might not be trusted to do so reliably.
- Provider Directory Service
 - The former Routing Service, which was conceived as a centralized directory of providers with their electronic addresses and protocols supported for various transactions, has now been replaced by an optional Provider Directory Service. Now, publishing and maintaining provider directories has been delegated to the entities (in accordance with certain interoperability standards), which means that there will be multiple provider directories instead of a single source. While entities may choose to use the Provider Directory Service, there is no obligation to do so.
 - One implication arising from this design is that in order to query for a provider without knowing the name of the entity beforehand would necessitate the searching of multiple directories. If so, this would likely have significant performance concerns. A question to be answered is whether there are technical solutions to adequately address these concerns, e.g. federating the directories so that a single query can be executed against all of the directories, or maintaining a central provider directory that mirrors the content of the distributed directories for purpose of querying.

Use Cases:

Walter then went through some example HIE use cases in the draft document that illustrate how the CS-HIE Services can be used to perform meaningful use functions. Please refer to the draft document for a detailed description of these use cases. The following comments were made by participants.

- Electronic transmission of structured lab results to EHRs
 - David Bass asked about the benefit of a laboratory using the CS-HIE Services to send results, if it likely already has the information pertaining to the ordering physician as part of the lab order. Walter pointed out that the contact information of the ordering physician could in some cases be out of date, which would result in the lab results not being sent to the correct address.
- Provide summary of care records for transitions of care
 - Paul Collins asked what happens to the transaction in the case that an error occurs somewhere, e.g., an assertion is not properly received. Walter clarified that depending on the policies of the receiving system with respect to assertions, the transmission may either be accepted or rejected. David Bass commented that it would be important to

think about how to handle errors in general, since errors are likely to occur on a regular basis.

- Paul Collins also asked whether it would be necessary for the EHR systems to interoperate with the CS-HIE infrastructure. Walter stated that this would be the most convenient way of interacting from the user's perspective; however, another possibility would be to use a web portal that is hooked into the CS-HIE infrastructure, which could then send a file to the receiving system.
- Submit electronic immunization data
 - Walter asked whether the proposed federated trust model where entities in the Entity Registry Service are trusted to authenticate their own users would be workable for CDPH's statewide immunization registry system that would be developed. Scott Christman replied in the affirmative, and that he would seek confirmation of this.
 - Paul Collins asked whether there would be standardization of messages to and from the various immunization registries. Scott answered that the immunization registries would be expected to comply with whatever standards are agreed upon and specified in the HIE infrastructure pertaining to immunization registries. Walter stated that in the current draft proposal, every entity that has an entry in a published directory for a particular transaction must support the standards specified for that transaction; however, the entity is free to support other means of performing the transaction as well if desired. There was agreement among the members on the call that this requirement was appropriate.

Identities and the Trust Framework

Walter briefly shared the current thinking on the types of identities required in the proposed system, which was shaped by discussions with one of the TWG co-chairs as well as individuals involved with the HL7 community. At present, there are three distinct types of identities that appear to be required:

- Information systems. These are nodes on the internet that can be reachable from any other system that wishes to exchange information. The addresses of these information systems are included in the directory entries. Digital certificates and private keys assigned to these nodes are needed for authentication, encryption, and integrity protection of the information exchanged.
- Legal entities. These are organizations that are willing to accept the legal responsibility for provisioning, credentialing, and authenticating their users. Legal entities are registered in the Entity Registry and are responsible for publishing accurate directory information. Legal entities sign authentication and authorization assertions on behalf of the principals engaging in HIE transactions.
- Providers (Principals). These are the senders of record and intended recipients of HIE transactions. The purpose of provider identities is to allow data trading partners to identify and locate intended recipients via provider directory entries, to enable recipients of HIE transactions to make authorization decisions, and to provide a record for logging and audit.

Walter will send out a detailed description of these identities to the group for comment and feedback.

Summary of Key Questions/Issues/Decision Points:

- Will the proposed federated trust framework engender sufficient trust among large organizations who have significant legal liability concerns to participate in HIE using the CS-HIE infrastructure?
- What technical solutions are there to enable a rapid distributed query of the multiple provider directories that will be published by entities and supported by the architecture?

Next Steps:

- Walter will send out a detailed description of the three distinct types of identities to the group for comment and feedback.
- Members of the group are encouraged to provide feedback on the latest draft of the technical architecture.
- The next meeting is scheduled for Wednesday 2/10/10, 11AM-12:30PM.

Members Present

Name	Organization
Dave Bass	CA Dept. of Health Care Services
Scott Cebula	Independent
Scott Christman	CA Dept. of Public Health
Paul Collins	CA Dept. of Public Health
Robert("Rim") Cothren	Cognosante, Inc.
Jeff Evoy	Sharp Community Medical Group
Daniel Haun	Adventist
Jen Herda	Long Beach Network for Health
Kathryn Lowell	CA Business, Transportation and Housing Agency
Lee Mosbrucker	CA Office of the Chief Information Officer
Eileen Moscaritolo	CalOptima
Orlando Portale	Palomar Pomerado Health District
Jim Thornton	MemorialCare
Kris Young	CA Office of Health Information Integrity

Staff Present

Name
Walter Sujansky
Peter Hung